UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, vs. MANUEL AGUSTIN RODRIGUEZ-SERNA Defendant.	CASE NO. 18cr3739 WQH ORDER

HAYES, Judge:

The matter before the Court is the motion to suppress fruits of illegal wiretap or in the alternative for a *Franks* hearing filed by Defendant. (ECF No. 40).

BACKGROUND FACTS

Beginning in 2017, Homeland Security Investigations (HSI) agents began an investigation into a suspected drug trafficking and money laundering organization operating in Ecuador, Colombia, Venezuela, Guatemala, Costa Rica, Mexico, and the United States. The investigators obtained the initial authorization to intercept a Blackberry PIN in February 2017.

In July 2017, agents identified screen name "RITA" who interceptions revealed coordinated movement of narcotics proceeds from the United States. Wiretaps identified Defendant as an associate of RITA.

On September 12, 2017, investigators requested initial authorization from the federal district court to intercept electronic communications, internet traffic, and electronic mail communications going to a particular Blackberry device assigned PIN 86218EB with no known subscriber under the screen name JAVIER MECANICO

("TBB#11"). (Ex. 3 at 5). The application and attached affidavit detailed the goals of the investigation and the investigative efforts to date. The application included technical details regarding the interceptions and specified that monitoring would occur in the Southern District of California. The application detailed minimization procedures that would be used and that communications not pertinent to the investigation would not be shared with the investigative team.

On September 13, 2017, United States District Court Judge John Houston issued an order granting the Title III wiretap application and authorizing the interception of electronic communications of TBB#11, for a period of 30 days.

On November 7, 2017, Judge Houston granted a new Title III application to intercept TBB#23, Screen Name "Caterpila," believed to be used by the Defendant, for a period of 30 days.

On December 20, 2017, Judge Houston granted a new Title III application to intercept TBB#25, Screen Name "Caterpilarr," believed to be used by the Defendant, for a period of 30 days.

On January 31, 2018, Judge Houston granted a new Title III application to intercept TBB#26, Screen Name "La Barca," believed to be used by the Defendant, for a period of 30 days.

On March 26, 2018, Judge Houston granted a new Title III application to intercept TBB#35, Screen Name "Charro," believed to be used by the Defendant, for a period of 30 days.

Each application included a probable cause statement, including relevant images intercepted. Each application detailed the progress of the investigation and addressed the necessity of the continuing interceptions to meet the goals of the investigation.

On April 18, 2018, all interceptions of Defendant ceased.

On August 22, 2018, an indictment was returned charging Defendant with international conspiracy to distribute cocaine in violation of 21 U.S.C. § 853.

On November 15, 2018, Defendant was arrested in Arizona and transferred to the

Imperial County Jail in El Centro, California. Defendant was arraigned by the United States Magistrate Judge and entered a plea of not guilty.

On May 28, 2019, Defendant filed a motion to suppress wiretap evidence, or in the alternative, for a *Franks*[1] hearing.

CONTENTIONS OF THE PARTIES

Defendant contends that the act of interception, the acquisition of communications contemporaneously with transmission in violation of the Wiretap Act, 28 U.S.C. § 2510 *et seq*., occurred in this case. Defendant asserts that the interception of his private text communications are subject to the statutory suppression contemplated by the Wiretap Act. Defendant asserts that the affidavits in support of the applications do not establish necessity as required by 18 U.S.C. § 2518(1)(c), and that the United States failed to comply with the minimization requirements of 18 U.S.C. § 2518(5). Defendant further contends that the applications fail to establish probable cause to believe that he was engaged in conduct that violated the laws of the United States. Finally, Defendant contends that the interceptions of communications outside of the United States exceeded judicial authority under the Wiretap Act.

The Government contends that each application and order complied with the requirements of the Wiretap Act. The Government further contends that the remedy of exclusion for a violation of the Wiretap Act is not authorized for electronic communications. The Government asserts that Defendant may seek suppression of electronic communications in this case based solely upon his rights under the Fourth Amendment to the United States Constitution. The Government asserts that the affidavits established probable cause and complied with all requirements of the Fourth Amendment. The Government further contends that all electronic communications were intercepted and monitored solely in the Southern District of California in compliance with the Wiretap Act and the orders of the district court.

[1] *Franks v. Delaware*, 438 U.S. 154 (1978).

RULING OF THE COURT

Application of the Wiretap Act, 28 U.S.C. § 2510 et seq.

In this case, government agents intercepted Defendant's Blackberry messaging (BBM). The parties agree that these interceptions are "electronic communications" under the Wiretap Act. Plaintiff United States contends that the statutory suppression scheme under § 2518(10)(a) does not apply. Defendant contends that the interceptions in this case were content communications contemporaneous with transmission and subject to suppression under the Wiretap Act.

While certain provisions of the Wiretap Act apply to "electronic communications," Defendant in this case has not shown that any violation of the statute occurred. *See* 18 U.S.C. § 2518(1). Even if a statutory requirement was violated, suppression for a statutory violation is not authorized under § 2518(10)(a) for an "electronic communication." 18 U.S.C. § 2518(10)(a).

Necessity

Wiretap authorizations are governed by the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510-2522. "To obtain a wiretap, the government must overcome the statutory presumption against this intrusive investigative method by proving necessity." *United States v. Rivera*, 527 F.3d 891, 897 (9th Cir. 2008) (citations omitted). The purpose of this requirement is to "assure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime." *United States v. Kahn*, 415 U.S. 143, 153 n.12 (1974) (citations omitted). The necessity requirement derives from 18 U.S.C. § 2518(1)(c) and (3)(c).

Section 2518(1)(c) provides that the affiant in support of an application for a wiretap must provide "a full and complete statement as to whether or not other investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(1)(c). A judge may approve a wiretap if he or she "determines on the basis of the facts submitted by the applicant that . . . normal investigative procedures have been tried and failed or why

they reasonably appear to be unlikely to succeed if tried or to be too dangerous . . . ." 18 U.S.C. § 2518(3)(c).

The "full and complete statement" requirement of Section 2518(1)(c) is satisfied where the affidavit provides "specific probative facts" which "show with specificity why *in this particular investigation* ordinary means of investigation will fail." *United States v. Commito*, 918 F.2d 95, 97-98 (9th Cir. 1990) (citation and quotation omitted). A judge must "determine that ordinary investigative techniques employing a normal amount of resources have failed to make the case within a reasonable period of time." *United States v. Spagnuolo*, 549 F.2d 705, 711 (9th Cir. 1977). However, "the government need not exhaust every conceivable investigative technique in order to show necessity." *United States v. Bennett*, 219 F.3d 1117, 1122 (9th Cir. 2000) (citation omitted).

The review of the court "includes an assessment of whether the affidavit attests that adequate investigative tactics were exhausted before the wiretap order was sought or that such methods reasonably appeared unlikely to succeed or too dangerous." *United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1111 (9th Cir. 2005) (citation omitted). The Court of Appeals has "adopted a 'common sense approach' in which the reviewing court uses a standard of reasonableness to evaluate the government's good faith effort to use alternative investigative means or its failure to do so because of danger or low probability of success." *United States v. Blackmon*, 273 F.3d 1204, 1207 (9th Cir. 2001) (citation omitted).

Each affidavit provided specific facts that detailed the progression of the investigation as a whole, as well as the successes and limitations of traditional methods used during the investigation. The affiant specifically addressed the use of confidential informants, physical surveillance, search and seizures, grand jury subpoenas, telephone records, and other traditional investigation methods. The affiant discussed cooperators, including specific pilots and detailed the limitations of their cooperation in accomplishing the goals of the investigation.

The affidavits met the requirements of § 2518(1)(c) and the Court did not abuse its discretion in finding the necessity requirement was met. The issuing judge reasonably concluded that the affiant made a sufficient showing that target devices were currently used in criminal activity, and that the continued intercept of target devices was necessary because "ordinary investigative procedures, employed in good faith, would likely be ineffective in the particular case." *United States v. McGuire*, 307 F.3d 1192, 1196 (9th Cir. 2002) (citation omitted). While the investigation had produced some results, the issuing judge reasonably concluded that the goals of the investigation had not yet been achieved, and that "ordinary investigative technique employing a normal amount of resources [would] fail to make the case with a reasonable time." *Spagnuolo*, 549 F.2d at 711.

Minimization

Defendant contends that there was not an adequate showing of minimization. The Government asserts that the authorization for interception of communications for the stated targets and described criminal activity was supported by the facts set forth in the affidavit.

Section 2518(5) requires that the Government conduct wire intercepts so as to "minimize the interception of communications not otherwise subject to interception . . . ." 18 U.S.C. § 2518(5). The Government has the burden to show minimization. *United States v. Torres*, 908 F.2d 1417, 1423 (9th Cir. 1990). In *Torres*, the Court of Appeals explained:

> Minimization requires that the government adopt reasonable measures to reduce the interception of conversations unrelated to the criminal activity under investigation to a practical minimum while permitting the government to pursue legitimate investigation. The standard for minimization is reasonableness.

Id. at 1423 (citations omitted). "The mere interception of calls unrelated to the drug conspiracy does not indicate a failure to meet the minimization requirement." *Id.*

In this case, the applications, affidavits, and orders contained minimization procedures. There are no facts to support the conclusion that any target of the

investigation or any goal of the investigation was not proper. Defendant does not provide a single interception which Defendant asserts should have been minimized or any suggestion that any minimization procedure was inadequate. The record demonstrates minimization efforts in accordance with 18 U.S.C. § 2518(5).

Defendant's request for training logs and minimization procedures is denied. *See United States v. Perez*, Case No. 10CR3044-WQH, 2011 WL 1259823, *5 (March 29, 2011) (concluding that minimization guidelines are not subject to disclosure under Rule 16(a)(2)).

Remedy of Statutory Violation

Each application, affidavit, and the order in this case specifically addresses the requirements for probable cause, necessity and minimization required under 18 U.S.C. § 2518. However, even if a statutory violation occurred, suppression for a statutory violation is not authorized for an electronic communication.

Section 2518(10)(a) provides:

> Any aggrieved person . . . may move to suppress the contents of any wire or oral communication intercepted . . . or evidence derived therefrom, on the grounds that—
> (i) the communication was unlawfully intercepted;
> (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
> (iii) the interception was not made in conformity with the order of authorization or approval.

§ 2518(10)(a) (emphasis added).[2] BBM data is "electronic communications," suppression is not permitted by the statute. *See United States v. Reed*, 575 F.3d 900, 915 (9th Cir. 2009) ("[T]here is no statutory remedy of suppression for interceptions of 'electronic communications.'"). However, Defendant is entitled to seek suppression of his communications based on alleged violations of the Fourth Amendment. *See* 18 U.S.C. § 2518(10)(c) ("The remedies and sanctions described in this chapter with

[2] Title III was amended in 1986, by the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986), to expand certain protections provided to wire and oral communications, to electronic communications. The ECPA did not expand the scope of the exclusion remedy in 18 U.S.C. § 2515 to include electronic communications.

respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.").

Fourth Amendment violation

Defendant contends that suppression is required on the grounds that the judicial officer could not find reason to believe that an individual named in the application was engaged in conduct that violated laws of the United States. Defendant asserts that the conversations described by the affiant could have just as reasonably involved legal activity. Defendant further asserts that the conversations involved pesos to be delivered in Colombia and lack any nexus to a violation of law occurring in the United States.

Plaintiff United States contends that communications from TBB#11 were initially intercepted coordinating the movement of narcotics proceeds with RITA. Plaintiff United States asserts that evidence of money laundering of narcotics proceeds is inextricably linked to narcotics trafficking. Plaintiff United States further asserts that the September 12, 2017 application and the previous application incorporated by reference established RITA's role as a high volume money broker for drug traffickers, facilitating drug trafficking in violation of 21 U.S.C. §§ 841(a)(1) and 959.

The Fourth Amendment not only commands that a warrant issue only "upon probable cause, supported by Oath or affirmation," but also requires that any warrant "particularly describe[s] the place to be searched, and the persons or things to be seized." *Berger v. New York*, 388 U.S. 41, 55 (1967) (quoting U.S. Const. Amend. IV). "In the wiretap context, those requirements are satisfied by identification of the telephone line to be tapped and the particular conversations to be seized." *United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977). In this case, each application presented to Judge Houston particularly described the conversations to be monitored and seized.

In order to find probable cause to issue an order authorizing interception of communication, the Court must determine whether there was a substantial basis for concluding that the electronic device to be tapped is being used to facilitate the

commission of a crime. "Probable cause means only a 'fair probability,' not certainty, and requires consideration of the totality of the circumstances." *United States v. Garcia-Villalba*, 585 F.3d 1223, 1233 (9th Cir. 2009) (citation omitted). The decision is made by the issuing court on the basis of practical, common-sense considerations and overturned only if lacking a "substantial basis." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). A review of the affidavits in this case clearly supports the determination that there was probable cause to issue the orders.

In the initial August 4, 2017 application, the affiant informed the district judge that law enforcement had identified a Blackberry device under the screen name "RITA" coordinating the movement of narcotics proceeds with an identified Mexican citizen working for a drug trafficking organization facilitating the movement of large amounts of narcotics proceeds. The affiant informed the district judge that he believed that RITA assisted the drug trafficking organization in coordinating the transportation and distribution of narcotics proceeds in the United States and other countries. The affiant detailed communications between the Mexican citizen and RITA discussing the movement of narcotics proceeds in Texas and Los Angeles.

In the September 12, 2017 application, incorporating the fact from the initial application, the affiant informed the district judge that wiretaps identified the user of TBB#11 as a close associate of RITA. The affiant outlined an intercepted Blackberry conversation on August 10, 2017 between TBB#11 and RITA believed to be coordinating a delivery of narcotics proceeds in Colombia. The affiant outlined a second conversation on August 11, 2017 believed to be confirming the delivery of narcotics proceeds in Colombian pesos. The affiant further informed the district judge of 962 electronic communications between TBB#11 and another individual believed to be involved in the shipment of narcotics intended for importation into the United States and the receipt of payments. The Court concludes that the information provided by the affiant detailed the investigation and provided probable cause to believe that the target subjects, including TBB#11, have committed and will continue to commit the described

criminal activity.

The September 12, 2017 order for interception of TBB#11 found probable cause to believe that the communications of TBB#11 and others were being used to facilitate offenses under 18 U.S.C. § 2516, such as distribution of controlled substances, importation of controlled substances, and money laundering. The facts in the affidavits provided the district judge with reason to believe that the offenses had a direct connection to the United States. The district judge had the authority to authorize the interceptions based upon the finding of probable cause to believe that the communications of TBB#11 and others were being used to facilitate the importation of controlled substances in violation of 21 U.S.C. § 959. *See Chua Han Mow v. United States*, 730 F.2d 1308, 1311 (9th Cir. 1984) (concluding Congress intended extraterritorial application of Section 959). An investigation into the coordination of narcotics proceeds is directly related to the violation of 21 U.S.C. § 959 which prohibits the distribution of controlled substances intended for unlawful importation into the United States. The district judge properly found probable cause to authorize the interception of electronic communications over TBB#11.

Extraterritorial interceptions

Defendant contends that suppression is required on the grounds that all intercepted communications were within Mexico, Venezuela, Guatemala, Costa Rica, and Colombia. Defendant asserts that he is a Mexican citizen; that the majority of his communications with other Mexican citizens occurred within Mexico; and that there was no coordination with the Mexican judiciary to conform with the requirements of Mexican law. Plaintiff United States contends that the government complied with all requirements of Title III and all electronic communications were intercepted and monitored solely in the Southern District of California.

In *United States v. Luong*, 471 F.3d 1107, 1109 (9th Cir. 2006), the Court of Appeals for the Ninth Circuit specifically addressed "[w]hat constitutes 'interception' within the meaning of section 2518(3)[.]" *Id.* The Court of Appeals stated: "We join

several of our sister circuits in holding that the district court had jurisdiction because the intercepted communications were first heard by the government within the court's district." *Id.; see also United States v. Cosme*, Case No. 10-cr-3044-WQH, 2011 WL 3740337 (S.D. Cal. 2011) (concluding that interceptions of defendant using a cellular phone in Mexico by monitors and equipment located in the Southern District of California were within the authority conferred by § 2518(3)).

The record shows that the district judge was informed that the target Blackberry devices have a Mexican service provider and that interceptions will only take place in facilities located in the United States. The record in this case conclusively establishes that the wireroom used in this investigation was physically located in the Southern District of California. All interceptions occurred in Imperial, California from February 2017 to April 2018; and in El Centro, California from May 2018 to June 2018. The intercepted communications were first read and minimized in the Southern District of California. The record establishes that all conversations were intercepted in compliance with §2518(3).

Franks hearing

In *Franks v. Delaware*, the Supreme Court examined the circumstances under which a defendant may "attack the veracity of a warrant affidavit after the warrant has been issued and executed." 438 U.S. at 164. "A defendant is entitled to a *Franks* hearing only if he makes a two-fold showing: intentional or reckless inclusion, or omission and materiality." *United States v. Bennett*, 219 F.3d 1117, 1124 (9th Cir. 2000). To make this showing, a defendant "must make specific allegations that indicate the portions of the warrant claimed to be false" and "[t]he allegations must be accompanied by a detailed offer of proof, preferably in the form of affidavits." *United States v. Kiser*, 716 F.2d 1268, 1271 (9th Cir. 1983) (citation omitted). In this case, Defendant did not identify any specific facts omitted and did not provide an offer of proof of any omitted facts necessary to a finding of probable cause. A *Franks* hearing is not required.

CONCLUSION

IT IS HEREBY ORDERED that the motion to suppress fruits of illegal wiretap or in the alternative for a *Franks* hearing (ECF No. 40) is denied.

DATED: September 5, 2019

WILLIAM Q. HAYES
United States District Judge